REMARKS

I. Status of Claims

Claims 1-3, 6-12, 14-24, 26 and 27 are pending in the above-identified patent application. Claims 1-3, 6-12, 14-24, 26 and 27 remain rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,298,445 issued to A. Shostack et al. (hereinafter "Shostack").

Applicants respectfully disagree with such rejection of all pending claims and traverse herein.

II. Status of Amendments

In response to the Amendment dated on July 26, 2004, the rejected of claims 1-3, 4-12, and 14-27 under 35 USC § 112, second paragraph, was withdrawn, and the rejection of claims 1-3, 5-12 and 15-27 as being anticipated by Shostack was maintained.

III. Summary of Invention

Applicants' claimed invention is directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host (associated with a first network) is probed with a particular packet, where the packet is intentionally configured with a source address which is associated with the second communications network, and the connectivity measure is determined as function of a response from the probed host (see, e.g., Applicants' Specification, page 4, line 27 – page 5, line 6; and page 8, lines 20-22) to the packet. Said another way, Applicants' claimed invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to a specifically configured probe packet. In brief, it is the determination of such connectivity measure, using the probe packet configured in accordance with the invention, that is the contribution advanced by the Applicants over the cited prior art.

IV. Issues

The one (1) issue presented for review is:

1. Whether claims 1-3, 6-12, 14-24, 26 and 27 are properly rejected under 35 U.S.C. §102(e) as being anticipated by Shostack?

V. Grouping of Claims

Applicants consider claims 1-3, 6-12, 14-24, 26 and 27 as a group which stand or fall together.

VI. Argument

Rejection of Claims under 35 USC § 102(e)

The Office Action rejected claims 1-3, 5-12 and 15-27 under 35 USC § 102(e) as being anticipated by Shostack. Applicants respectfully disagree and submit that each of the currently pending claims is patentably distinct from Shostack.

As outlined in the prior Amendments submitted by the Applicants, heretofore, the well-known use of "spoofed packets" (by unauthorized users or hackers) is directed to gaining illegal entry into a secure system. To be clear, as stated previously, the Applicants recognize that "spoofing", i.e., the faking of the sending address of a transmission in order to gain illegal entry into a secure system (see, e.g., a general definition available at http://www.techweb.com/encyclopedia; or Shostack at column 1, line 64 – column 2, line 3) is not new. Indeed, Applicant William Cheswick in the subject Application is a recognized Internet security expert (see, e.g., the references enclosed with the Amendment, dated April 7, 2004) intimately familiar with spoofing and spoofed packets. Heretofore, the well-known use of spoofed packets (by unauthorized users or hackers) is directed to gaining illegal entry into a secure system.

In contrast, Applicants have realized that spoofed packets can serve different purposes (and non-malicious) by providing an enhanced security tool for discovering the connectivity between networks. This connectivity measure, in turn, can be used by

system administrators to prevent malicious attacks (including but not limited to malicious spoofing). It is at least this aspect of Applicants' invention that stands in stark contrast to the cited Shostack passages (i.e., Shostack, column 12, lines 41-57; and column 13, lines 1-5), and anything else therein, in the instant rejection of Applicants' claims.

Specifically, in addition to the discussion of Shostack in the prior Amendments, Applicants' respectfully submit that Shostack teaches a technique for testing for susceptibility to various so-called security vulnerabilities, such security vulnerability including IP spoofing. For example, Shostack at column 12, lines 50-55 describes an aspect of Shostack's technique which "...probes the ports of each of the IP devices for programs that contain security vulnerabilities that may be exploited...". Shostack's "security vulnerabilities", as referenced throughout such disclosure, are of the type listed in Shostack's Table 1 (see, e.g., Shostack, columns 5 and 6). While it is true that one such Shostack security vulnerability is a "check of the firewall for IP spoofing" (see, Shostack, column 5, lines 59-60) or "...assess the security vulnerabilities of a remote computer connected to the network..." (see, Shostack, column 13, lines 2-3), these are not disclosures which are fatal to the novelty of Applicants' claimed invention. That is, Shostack's teaching with regard to such IP spoofing is checking whether a particular firewall (see, e.g., Shostack, firewall 12 in FIG. 1) or remote computer is vulnerable (susceptible) to IP spoofing.

In support of the outstanding rejection of Applicants' pending claims, the Office Action on page 3 includes:

> "...Examiner would like to point out the teachings in Shostack in column 13 starting at line 1. Shostack teaches a fourth module of his system which allows a remote computer to first connect to a network service and like the second network module, interrogates the service. Examiner references column 12, lines 41-57 as the teaching of what module two does. Specifically module two carries the network scan and generates a map of the network and scans the ports for known security vulnerabilities. Therefore module four does this from a remote location. The remote location would then have a source address associated with a second communications network. An address that is different from the first communications network. (Emphasis added by Applicants); and
>
> "Shostack also teaches a sixth module which is a communication module that allows an integrated security system to communicate with a

> similar system over a computer network. In line 27, the module invokes remote systems. In line 34, Shostack teaches that this sixth [module] checks the integrity of the service connection. This teaching is another example of communication between networks to perform the security functions of Shostack's invention.." (emphasis added by Applicants); and
>
> "The Examiner has pointed to two separate teachings where Shostack teaches or suggests utilizing a probe packet to determine a connectivity measure between the two communication network where the packet includes a source address which is associated with a second communications network..."

Respectfully, the Applicants submit that the Examiner reading of Shostack on the currently pending claims, as amended previously, is misplaced. First, at the risk of being repetitive, the Applicants recognize that spoofing, network census compilations and port scans are not new. Second, Applicants submit that Shostack's second module (and, for that matter Shostack's fourth module) as highlighted in the Office Action is not performing (and does not anticipate, teach or suggest) Applicants' claimed invention. In particular, the fact that Shostack's fourth module essentially implements—on a remote basis—the functionality of the second module does not teach or suggest Applicants' claimed invention. Shostack, at column 12, lines 41-55, teaches:

> "...The second module 76 accesses the database of security vulnerabilities 92 and assesses network security. The second module 76 connects to a network service, accepts information from the service and interrogates the service. The second module 76 performs a network scan and...The network scan produces a map of the network 86 which is essentially an inventory of the Internet Protocol (IP) devices connected to the network. Using network protocol, the integrate system also probes the ports of each of the IP devices for programs that contain security vulnerabilities that may be exploited.. The network scan ensures that the network 20 and a local server 18 is protected against any unauthorized access that may penetrate the firewall 12...."

Again, the Office Action is relying on the above features of Shostack's second module and the "remote" action of Shostack's fourth module to support the rejection of Applicants claimed invention. Applicants do not dispute that Shostack's fourth module allows a remote computer to first connect to a network service then accepts information from the service and like the second module also interrogates the services (see, e.g., Shostack, column 13, line 3-6). Applicants do dispute, and disagree with, the suggestion that such teaching anticipates the claimed invention herein. Applicants' claimed

invention is directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host (associated with a first network) is probed with a particular packet, where the packet is intentionally configured to include a source address which is associated with the second communications network, and the connectivity measure is determined as function of a response from the probed host to the packet. Said another way, Applicants' claimed invention is directed at discovering—as function of the sending/receiving of the claimed probe packet—connectivity of, or between, a host machine (or host machines) not whether such host (or hosts) is susceptible to IP spoofing.

Shostack's second and fourth modules may be used to determine whether a service engaged by a host computer (including a remote host) is vulnerable to a known set of security vulnerabilities (in particular, Shostack's "security vulnerabilities 92"). Neither of these modules employs the configured probe packet, as claimed by Applicants, to determine a connectivity measure between two communication networks (where the packet includes a source address which is associated with a second communications network) which can be used to identify potential unsecure or rogue connections between a probed host (of a first communications network) and some other host on a second communications network. As pointed out previously, Applicants appreciate the Examiner's thoroughness in pointing out in the Office Action that the claimed invention does not specifically recite the term "spoofed probe packet" but fail to fully understand the relevance in sustaining any rejection to Applicants' pending claims. That is, Applicants' claimed invention does include the limitation of probing a host of a first communications network with a particular packet, where the packet includes a source address which is associated with a second communications network. Applicants have particularly pointed out and distinctly claimed the subject matter which Applicants regard as the invention. While such a claim recitation may be understood by those skilled in the art as having similar features to a "spoofed packet", it may include other types of probe packets which have the claimed limitations of Applicants invention.

Further, Shostack's sixth module teaches a "communications module" which performs well-known system functions such as maintaining communication between Shostack's modules and/or other similar systems, database sharing, report generation/analysis, security and checking the integrity of existing service connections (see, e.g., Shostack, column 13, lines 18-36). As detailed above, Applicants find no teaching or suggestion in Shostack's sixth module with respect to the aspect of Applicants' claimed invention directed to utilizing a probe packet to determine a connectivity measure between two communication networks (where the packet includes a source address which is associated with a second communications network).

Regarding the rejection of each of the presently pending dependent claims these claims depend ultimately from one of the pending amended independent claims 1, 10, 16, 21 and 24 herein which Applicants submit are patentably distinct over Shostack for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending amended independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Shostack for the aforesaid reasons, as well as other elements these claims add in combination to their base claim.

Therefore, in view of the foregoing, Applicants respectfully submit that each of the currently pending independent claims, as amended, is patentably distinct from Shostack. As such, it is respectfully submitted that each of the currently pending claims in the application is in condition for allowance and reconsideration is requested. Favorable action is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Steven Branigan
Hal Joseph Burch
William R. Cheswick

By _____
Donald P. Dinella
Attorney for Applicants
Reg. No. 39,961
908-582-8582

Date: 11/23/04

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030